Professional Access Control

Leigh de la Motte and Jacky Hartnett
University of Tasmania

Abstract

Topic area and paper objectives:
This paper investigates the hypotheses that it is possible to build a practical access control system for patient records within a hospital domain that ensures access to all those who are at any one time part of a particular patient's treating team yet at the same time provides appropriate barriers to access for those not currently part of this team. A caveat for this hypothesis is that at no time should a clinician be barred from access to a particular record, but that means should exist to ensure that appropriate access is accepted and inappropriate access reported upon. Central to this idea is that it should be possible to use standards of professional ethics and normal workflow to enable the model.

Background and concise literature review:
Traditional models of access control do not cope well with the problem of how to define access permissions for a team that is dynamic in nature (as is a treating team) and where the access is to objects (patient records) only in the loosest sense 'owned' by those who have a need to access such objects. In these models either the system administrator has to define permitted access in advance (mandatory access control) or the owner of the data can define the permitted accesses (discretionary access control) (Pfleeger 2000). Extensions to Role Based Access Control (RBAC) and Team Based Access Control (TMAC) have provided the most useful solutions to date but still require a system administrator or surrogate to define appropriate access in advance. (Ferraiolo & Kuhn 1992) (Ramaswamy & Sandhu 1998) (NIST 2004) (Thomas 1997) (Georgiadis et al 2001) (Georgiadis 2002) However, work by Thomas & Sandhu (1997) and Alotaiby & Chen (2004) has shown that it is possible to incorporate changes to access privileges as part of normal workflow.

Methods:
As a result of observing and discussing normal and unusual workflow patterns within the Tasmanian hospital environment a set of scenarios were developed each of which characterised a unique instance of change to whom should be able to access a patient record. The method used by current access control models to handle each scenario was then analysed. A new definition of a team in a hospital environment was then used to develop the Professional Access control (PAC) model that was implemented and tested in Oracle. Testing was carried out using each scenario in a simulated hospital of 3 wards, 20 staff and 20 patients.

Results and discussions:
Clinicians at a hospital were defined as either being Members: part of a patient's treating team, Colleagues: having the same role and belonging to the same unit as the patient or Associates: part of the hospital but not currently related to the patient. Being a team Member can be adjusted as part of the normal hospital admission and referral processes. Emergency access is provided subject to retrospective approval and auditing procedures. The model has been developed as an Oracle implementation for a simulated hospital environment and tested against the 24 scenarios defined. The Professional Access Control model allows for dynamic definition of the treating team and facilitates guaranteed availability to clinicians appropriate to their relationship to a patient. This is made possible by relying upon the professional ethics of clinicians rather than those of system administrators. It relieves the burden of predefining access control from system administrators without endowing clinicians with unnecessary system administration privileges.

1. Introduction

It is simple to state that the 'treating team' should have access to the records for a particular patient, but it has been hard to demonstrate that there is practical way to build computer systems to enforce this principle whilst at the same time ensuring that any legitimate access request is always granted, even in an emergency. Central to the difficulty is the fact that the definition of a treating team is fluid and can change in a manner that cannot be predicted in advance. This means that solutions have placed unrealistic requirements on system administrators as they attempt to predict what should be the authorised access patterns. This paper describes a solution that lifts the burden of defining the current treating team from the system administrator, instead capturing the changing access permissions as part of current workflow enabled by trust in the professional ethics of clinicians.

Computer security is much more than just a technical IT access problem. The largest security weaknesses in IT systems are often the people in the system (Schneier 2000, p.255). With paper records it has been traditional for hospital administrators and health professionals to guard access to patient records. The patient record is generally left with the patient in the hospital and any access to it is normally in view of the patient or other staff members. In contrast, with computer systems, it has been traditional for the system administrator to have control over who accesses which records. The emergence of digital health records therefore creates a "professional control" issue. Who should manage access to digital health records – the system administrator, the health professionals, or both?

The vast majority of Health professionals pride themselves on their ethical practice. Being a professional entails conformity to regulations, professional codes of behaviour, and relevant organisational policies. Breaches of these standards can result in severe personal repercussions. The very reason why it is uncommon for system administrators to be corrupt is because they are professionals and there are consequences if they are found wanting. There is no reason why health professionals should behave more irresponsibly given that they are informed of their responsibilities and that the system supports appropriate security policies.

The ideal access control model for the hospital environment would, it is suggested, give health professionals 100% guaranteed access to all relevant records while maximising confidentiality and integrity safeguards. This all needs to be done in a fashion that minimises implementation and running costs, and maximises system usability. Efficiency is maximised if the users can authorise each other to perform accesses, without the need to directly involve system administrators. This, in most aspects, reflects how the paper-based record system operates. System administrators should be left to do the high level tasks rather than being dragged onto the wards to do the patient-user and user-user authorisation tasks.

2. Methodology

The project consisted of seven stages: Workflow Analysis, Model Analysis, Team Definition, Model Development, Model Implementation, Functional Testing, and Scenario Verification.

Workflow Analysis was performed by interviewing health practitioners, administrators and IT managers. The purpose was to describe as many relevant and distinct hospital system requirements (in the form of scenarios) as practicable. Model Analysis involved researching related work in access control techniques and models. The purpose was to extract useful concepts from existing models that could be incorporated into a new model. A team-based access control model requires the team concept to be defined. The scenarios produced by the workflow analysis and the team-

based examples researched in the model analysis were analysed qualitatively to produce a suitable Team Definition for the hospital domain.

In the light of the information gleaned from the first three stages, the Model Development stage involved the definition a new access control model. The model had to meet the requirements of the Workflow Analysis and incorporate the useful features of existing models in a way that facilitated the team type defined in the third stage. The Model Implementation was done using Oracle, primarily because it was already in use in the Tasmanian *Department of Health and Human Services* (DHHS) controlled public hospitals.

Functional Testing of the implementation was performed using a software simulation of a hospital with 3 wards, 20 patients and 20 staff. This was necessary as it was impractical to pursue a clinical implementation before demonstrating the potential of the new model. The purpose of the functional testing was to ensure that the implementation possessed the functionality required and that correct authorisations were always maintained. Scenario Verification was performed as a double check to verify that the functionality required by the scenarios generated in the Workflow Analysis was indeed achieved. This meant checking the functionality requirements of each scenario individually.

3. Results

Workflow Analysis

The Workflow Analysis yielded a total of 24 scenarios. These scenarios were divided into five categories: Patient Issues, Staff Change Issues, Staff Information Issues, Administrative Issues, and Security Incidents.

Model Analysis

In order to find a model suitable for the volatile hospital environment, many existing access control models were investigated. The most significant of these included Role-Based Access Control (RBAC), TeaM-based Access Control (TMAC), Task-Based Access Control (TBAC), Organisation Based Access Control (ORBAC), Provision-Based Access Control (PBAC), and the Clark-Wilson Model. Auditing and middleware solutions were also investigated.

Middleware (Woodcock & Gillies 2003) (Hartnett 2002) and ORBAC (Kalam et al. 2003) were too complex for the envisaged solution. TBAC (Thomas 1997) and TMAC (Alotaiby & Chen 2004) showed that it was possible to use normal workflow operations to trigger access control functions. The solution can use this principle to allow behind-the-scenes access control.

Both RBAC (Ferraiolo & Kuhn 1992) (Ramaswamy & Sandhu 1998) (NIST 2004) and TMAC (Thomas 1997) (Georgiadis et al. 2001) (Georgiadis et al. 2002) are based on Mandatory Access Control (MAC). They therefore fundamentally require that privileges be specified by systems administrators in advance. In order to facilitate some predictable emergency access requirements they tend to either specify privileges which are too broad, or enable users to take on granting privileges which are designed for use by system administrators. Such user grants, it can be argued, are inconsistent with the definition of roles as well as dangerous from a security point of view.

The solution needs to overcome these RBAC/TMAC/MAC limitations by giving appropriate responsibilities to users in professional environments and by employing retrospective access control techniques similar to those proposed in PBAC (Kudo 2002). It can benefit by using a more fine-grained approach to team definition than that employed by TMAC. The solution must guarantee availability, while maximising confidentiality and integrity protection through improved granularity

of control. Reporting procedures can allow peer-review and auditing procedures to play a part in access control, making access control more than just a technical issue.

Team Definition

The three main features of the Professional Access Control (PAC) Model's team concept are that:

1. Each patient has their own personal team;
2. There are no team specific roles – roles are organisation wide; and
3. Each team is supported by two layers of backup personnel.

The one-to-many patient-team relation offers the most fine-grained solution and is superior to the many-to-many relations used in other team-based models. PAC teams are initialised automatically as part of the process of admitting a patient to a ward. This is achieved by having a *default team* for each ward. Default teams are defined by specifying a *default role set* for each ward. Each default team is then generated by automatically placing all staff members with the specified default roles who are able to work on the ward, on the patient's team.

The second point relates to staff roles. PAC uses the same concept of roles as RBAC. This means that staff can have multiple roles and generally more than one staff member has a particular role. PAC also uses a location context constraint called a *unit*. Each staff member has what is called a *unit set*, which is the group of units on which the staff member is currently allocated to work.

The unique feature of the PAC team concept is outlined by the third point. Once a team is defined for a patient, there by definition exist two further groups of staff which may be called upon to care for the patient. These further groups are defined by the relationship they have with the members on the patient's team. Figure 1 shows the team group and the two supporting staff groups.

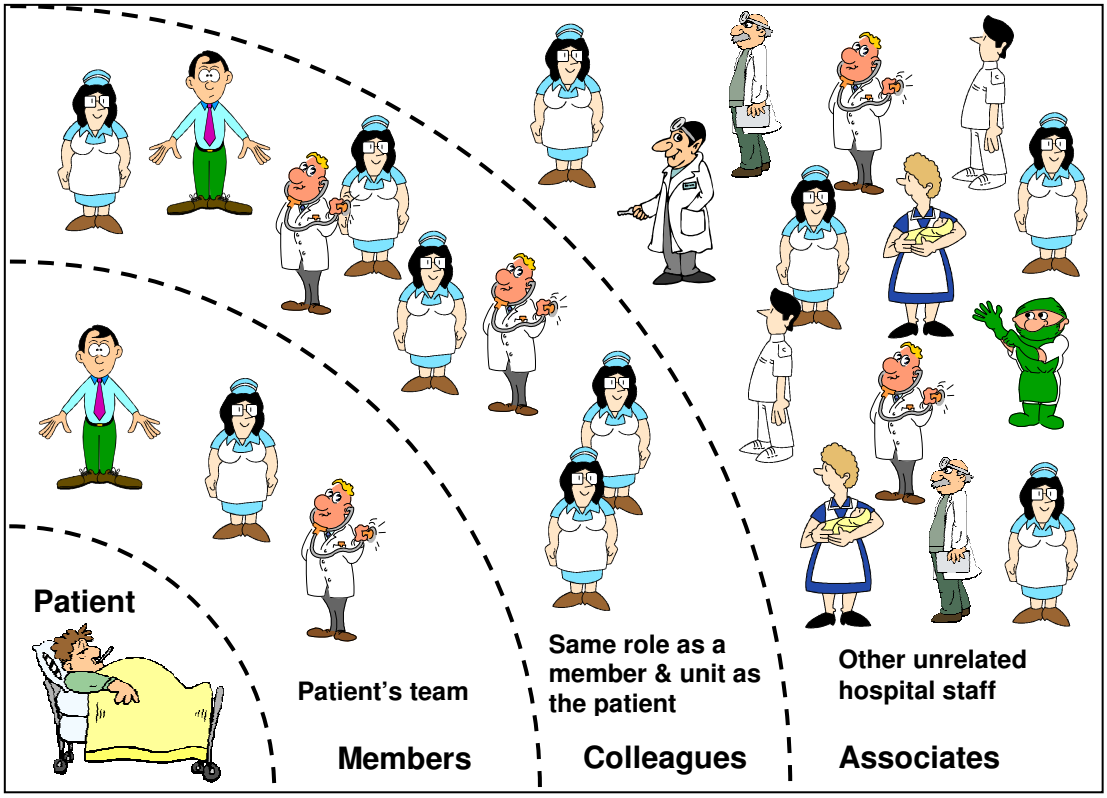

Figure 1: PAC Team Staff Categories

Staff members on the team are defined as *members*. Staff members who share a role with any of the team members and are allocated to work on the patient's unit are defined as *colleagues*. The remaining staff members, those who are neither members nor colleagues, are defined as *associates*. From a particular nurse's point of view, they may be a member of 6 patient teams; a colleague of 20 other patient teams; and an associate of 200 further teams.

PAC defines these three staff categories in order to allow different access control procedures to be used, depending on the closeness of a staff member to the patient in question. Access needs to be controlled on a need-to-know basis. Team members have the greatest need for access; colleagues may need access to help members in the normal course of work; and associates should only need access in exceptional circumstances. Access control should therefore be tight for associates, moderate for colleagues, and easy for members.

This team model allows PAC to be extremely flexible. It can easily cater for situations where the team structure varies from ward to ward in a hospital, or even for different supervisors using different approaches on the same ward, or different approaches to be taken on a per patient basis! A supervisor can make everyone on the ward a member of all patient teams, in one extreme. Conversely, at the other extreme, they can restrict access down to having only one carer for a patient. The approach used for a patient can be changed at any time. This flexibility is in stark contrast to the team structures used in TMAC models, and makes PAC-based systems highly usable.

Model Development

Professional Access Control (PAC) is a high level team-based access control model which incorporates Trusted Access Control (TAC) (de la Motte & Hartnett 2005), RBAC and PBAC. It is designed to be used in domains such as hospitals where the users are professionals and have a clearly defined duty of care to the information owners (their patients). The priorities of the model are to guarantee availability and to minimise administrative overheads.

Figure 2 shows the main concepts of the model. The objects in the diagram represent the collection of one or more objects owned by the owner. In the hospital domain the objects would represent different parts of the patient's record. Members on the patient's team can directly access the record of the patient.

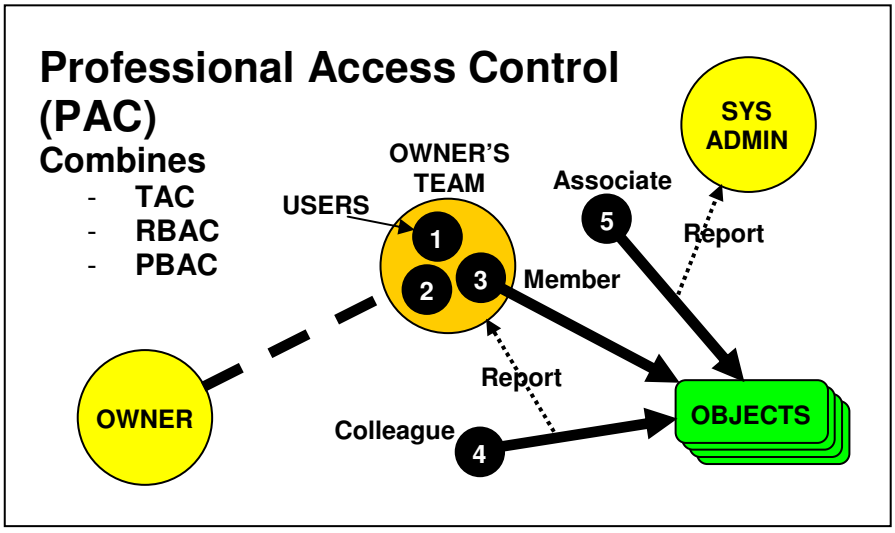

Figure 2: PAC Access Control Mechanisms

PAC incorporates TAC, RBAC and PBAC. TAC is the method used to add additional members to the team. Under TAC, any team member can add another user to the team. This is akin to a patient referral and is done without the need to involve the system administrator. RBAC roles are used in connection with a location context constraint to automatically initialise team membership on patient admission, as well as to determine the colleague user status. RBAC is also used to determine which parts of the patient's record is available to the accessing user. RBAC restrictions can be overridden in emergencies. PBAC is used to provide a reporting mechanism to deal with accesses by colleagues and associates. Accesses by colleagues are reported back to the team member(s), while accesses by associates are reported back to the system administrator.

The mechanism for adding users to the team is very simple. The vast majority of accesses are therefore made by team members. Accesses by colleagues and associates are in the minority. The reporting mechanism can be made to fit in with normal communications processes and therefore does not add any significant administrative burden. The system administrator has only a secondary access control role, that of monitoring accesses and merely checking a few of the more unusual accesses. The administrative burden on the system administrator is therefore reduced.

Model Implementation

The result of implementing the PAC model in Oracle was the *Oracle PAC Toolkit*. The toolkit is made up of two components – a set of database tables and a set of PL/SQL procedures and functions. All the PAC functionality is provided in top level PL/SQL procedures, while the data necessary for access control is stored in the database tables. While system administrators may choose to manipulate the tables directly, or through the Oracle Enterprise Manager, applications which use the toolkit only need to access the top level procedures. The tables are thus protected from applications and their users by Clark-Wilson style well-formed transactions.

Functional Testing

The functionality of the PAC implementation was tested by ensuring the procedural calls initiated the correct sequences of functional calls. A simulation was set up in the Oracle database of a hospital with wards, administrators, health practitioners and patients. The procedures were tested to ensure that the security state of the hospital remained valid. The results yielded no errors and showed that the desired functionality was being achieved.

Scenario Verification

It was shown that the model was able to meet the requirements of the 24 scenarios established in the Workflow Analysis stage.

4. Discussion

Much research has been done into developing access control systems for health related environments. Even after all this work, no clear system has emerged that meets the requirements in an efficient way. Many sophisticated and clever solutions have been developed, and while many of them have shown promise, there has been a tendency to reject them on the basis that they are either too inflexible or hard to implement. The aim of this project was to try to find a simple, low-impact solution to the access control problem which can be incorporated into hospitals.

PAC provides a workable solution that guarantees the availability of records to clinicians and therefore ensures they are never denied access to information necessary for clinical decision making. It achieves this without introducing any additional work for users, by allowing workflow

applications to trigger access control responses. The solution provides a system which can easily be implemented and that gives access to users on a need-to-know basis. The fine granularity of control increases confidentiality and integrity protections over existing solutions. PAC is very flexible, facilitating the formation of ad hoc treatment teams in a user friendly fashion.

PAC also reduces the burdens on the systems administrator and gives the appropriate level of responsibility to the clinical professionals who are most aware of the matters of patient confidentiality. It recognises the highly ethical environment in hospitals and adopts a peer-review process which is appropriate for the management of professionals. The flexible solution achieved by PAC is in stark contrast to the purely technical solutions that are currently on offer.

5. Conclusion

Initial studies into the health and hospital domains highlighted that for a system to be usable, access control mechanisms must guarantee the availability of patient information to practitioners. It was found that there were no existing access control models which could suitably guarantee availability in a volatile environment.

It was argued that in highly ethical environments, where there are adequate professional incentives to induce proper behaviour, there is fundamentally no reason why informed users should have a direct role in access control. In view of this, a new high level access control model, named Professional Access Control (PAC) has been proposed.

This paper proposes the Professional Access Control (PAC) Model. PAC is a user-controlled model which applies fundamental and proven techniques from existing access control models. It provides a flexible team concept which gives team members direct access to a patient's records, while allowing non-members to gain access through an efficient monitoring process. PAC provides primary control to the health practitioners, thus alleviating their dependence on system administrators to solve their access problems. As such it takes a great load off the system administrators, leaving them free to concentrate on other activities.

References

Alotaiby, F. T. and Chen, J. X. 2004, 'A Model for Team-based Access Control (TMAC 2004)', *International Conference on Information Technology: Coding and Computing (ITCC'04)*, IEEE, Las Vegas, Nevada, USA

de la Motte, L. H. and Hartnett, J. 2005, 'Trusted Access Control', submitted to *Australasian Conference on Information Security and Privacy (ACISP'05)*, Brisbane, Australia

Ferraiolo, D. and Kuhn, R. 1992, 'Role-Based Access Control', *15th National Computer Security Conference*

Georgiadis, C. K., Mavridis, I., Pangalos, G. and Thomas, R. K. 2001, 'Flexible Team-Based Access Control Using Contexts', *SACMAT '01*, ACM, Chantilly, Virginia, USA, pp. 21-27

Georgiadis, C. K., Mavridis, I. K. and Pangalos, G. I. 2002, 'Programming a view-based active access-control system for healthcare environments.' *Health Informatics Journal (2002)*: 191-198.

Hartnett, J. 2002, Research into the Implementation of Electronic Consent for the use of Patient Identifiable Health Data, University of Tasmania - School of Computing.

Kalam, A. A. E., Baida, R. E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C. and Trouessin, G. 2003, 'Organisation based access control', *4th International IEEE Workshop on Policies for Distributed Systems and Networks*, IEEE, Lake Como, Italy, pp. 120-131

Kudo, M. 2002, 'PBAC: Provision-based access control model.' *International Journal of Information Security* 12: 116-130.

NIST 2004, *Role Based Access Control*. viewed 6th October, 2004, <http://csrc.nist.gov/rbac/>

Pfleeger, C. P. 2000, *Security in Computing*, Prentice Hall PTR, Upper Saddle River, New Jersey.

Ramaswamy, C. and Sandhu, R. 1998, 'Role-Based Access Control Features in Commercial Database Management Systems', *21st National Information Systems Security Conference*, Crystal City, Virginia, USA

Schneier, B. 2000, *Secrets and Lies*, John Wiley & Sons, Inc., New York.

Thomas, R. K. 1997, 'Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments', *RBAC '97*, ACM, Fairfax Va USA, pp. 13-19

Thomas, R. K. and Sandhu, R. S. 1997, 'Task-based Authorisation Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorisation Management', *IFIP WG11.3 Workshop on Database Security*, Chapman & Hall, Lake Tahoe, California, USA

Woodcock, D. and Gillies, I. 2003, 'Generic middleware as a new paradigm for providing a single user interface to multiple disparate web-based clinical applications', *HIC 2003 RACGP 12CC Combined Conferences*, Darling Harbour, Sydney Australia